Rethinking the Approach to Consumers and Personal Data in the Digital Economy: Opportunities of Individual Control and Collective Redress

Laura Somaini

I. Introduction

The EU legal framework has set a high bar for the fundamental right to data protection – not least by adopting what is now a global golden standard, the GDPR.[1] In practice, however, it can be difficult to reconcile this right with the complex reality of data collection and use practices. Against this backdrop, this essay proposes the most beneficial (and realistic) way to frame a consumer-personal data relationship (Section II). It then argues the necessity to shift towards a holistic approach to data protection, competition and consumer law in the digital economy's context (Section III). Finally, this essay points out the opportunities of consumer collective redress and stakeholders' role (Section IV). Section V concludes.

II. Individual control over personal data and data portability

Individual control is necessary to entertain any kind of relationship with one's personal data. Years ago, scholarship warned that claiming control over personal data, was simply "delusional".[2] The concept, stemming from informational self-determination,[3] is understood as the ability of individuals to make meaningful choices regarding the use of their personal data.

In between the opposite ends of a *laissez-faire* attitude and the establishment of a proprietary paradigm, individual control is the most beneficial approach because it empowers individuals in the market, whilst still providing certain safeguards and protection vis-à-vis significant information and power asymmetries. Strict "propertization" of personal data, on the other hand, would not be compatible with the current framework[4] – nor advisable in the writer's opinion – due to data's non-rivalrous nature and the human rights rationale underlying data protection in the EU.[5] In the words of Stefano Rodotà: "the right to data protection has to do with one's personality – not one's property".[6]

In fact, the data protection reform endorsed the idea of individuals "reclaiming control over data".[7] Effective control relies on the provision of complete and transparent information about data processing practices – a lesson learned from consumer protection law. A first type of control is exercised at the initial stage of data approval and primary use, ensured by the GDPR through the conditions for valid consent and information, access, erasure, restriction and objection rights.[8]

---

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("GDPR").

[2] B. J. Koops, 'The trouble with European Data Protection Law', *International Data Privacy Law*, 4(4), 2014, 251-253. In the context of monopolies, C. Kuner *et al*., 'When two worlds collide: the interface between competition law and data protection', *International Data Privacy Law*, 4(4), 2014, 247.

[3] German Constitutional Court, *Population Census* (Judgment, 15 December 1983), BverfgE 65, 1, 41.

[4] N. Purtova, *Property Rights in Personal Data. A European Perspective*, Wolters Kluwer, 2012, 219-220.

[5] Article 8, EU Charter of Fundamental Rights.

[6] S. Rodotà, 'Data Protection as a Fundamental Right', in (eds.) S. Gutwirth *et al*., *Reinventing Data Protection?*, Springer, 2009, 81.

[7] Commission Communication, "A comprehensive approach on personal data protection in the European Union", COM(2010) 609 final, 7.

[8] I. van Ooijen, H.U. Vrabec, 'Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective', *Journal of Consumer Policy*, 42, 2019, 94, 100.

Relating to the secondary stage of data use,[9] the GDPR introduced the novel right to data portability.[10] This type of control establishes the entitlement to have personal data transferred back to the data subject or to another data controller in an automated and machine-readable format. The latter ensures not just accessibility, but meaningful re-usability of datasets.[11] Furthermore, data portability reduces lock-in effects,[12] allowing consumers greater choice among products and services. It enables user/consumer mobility as they can "take their profile and leave" in favor of a competing provider.[13] Therefore, organizations are incentivized to improve quality and prices of their offers to retain customers through effective competition and innovation, rather than artificially.[14]

Moreover, data portability is an example of how data protection, competition and consumer law intersect, highlighting the "multi-hatted" characterization of individuals in the context of the digital economy. This acknowledgment owes much to Giovanni Buttarelli's vision of a modern and fit-for-purpose data protection framework, following the EDPS' seminal Opinion on "Privacy and competitiveness in the age of big data".[15]

To date, data portability's potential to create a "user-centric digital environment"[16] remains largely untapped. Along these lines, the EU Data Strategy signaled the intention of enhancing such right by possibly imposing stricter requirements on interfaces for real-time data access and compulsory machine-readable formats in the context of certain products and services, such as smart home appliances or wearables.[17]

Bringing the right to data portability to fruition will corroborate control. Ideally, consumers are granted the freedom to make meaningful consumerist and privacy-related choices in the market, protect their prerogatives, challenge wrongdoing and seek remedy. Accordingly, effective control rights hold the promise for consumers to "share the wealth" of big data.[18] To achieve this goal, a comprehensive approach to the individual's role in the digital economy is necessary.

III. A holistic approach to data-related concerns in the digital economy

Consumer data has become a fundamental resource at the very heart of the most successful and innovative business models of the last decades. In this context, consumer data may constitute a driver and object of commercial practices that may well be caught in the scope of competition law.

Most recently, the proposed *Google/Fitbit* merger triggered a "phase II" control by the European Commission and raised, among others, concerns about data protection. As described by the Commission, by acquiring Fitbit, Google would amass (i) Fitbit's database containing information about its users' health and fitness; (ii) the

---

[9] *Ibid*., 102.

[10] Article 20, GDPR.

[11] L. Somaini, 'The right to data portability and user control: ambitions and limitations', *MediaLaws*, 3, 2018, 164-190; O. Lynskey, 'Aligning data protection rights with competition law remedies? The GDPR right to data portability', *European Law Review*, 42(6), 2017; P. Swire, Y. Lagos, 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique', *Maryland Law Review*, 72(2), 2013; I. Graef *et al*., 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law', Tilburg Law School Research Paper No. 2017/22.

[12] Commission Staff Working Document, Impact Assessment, SEC(2012) 72, 28.

[13] However, article 20 GDPR suffers some limitations: it applies only when processing is based on consent or on the performance of a contract; and does not cover derived and other secondary data. See Somaini, *cit.*, 'The right to data portability and user control', 186-187.

[14] Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, SWD(2017) 2 final, 47; B. Engels, 'Data portability among online platforms', *Internet Policy Review* 5(2), 2016, 6-7.

[15] "Preliminary Opinion of the European Data Protection Supervisor Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy", 2014.

[16] P. De Hert *et al*., 'The right to data portability in the GDPR: Towards user-centric interoperability of digital services', *Computer Law & Security Review*, 34(2), 2018.

[17] Commission Communication, "A European strategy for data", COM(2020) 66 final, 20-21.

[18] Article29 Working Party, Opinion 3/2013 on purpose limitation, 2 April 2013, WP203, 47.

technology to develop a similar database.[19] Google's commitments, as reported by the Commission, intended to create a data silo in order to store separately data collected via wearable devices from other Google datasets – with the specific restriction of using Fitbit's dataset for Google's advertising purposes.[20] Notwithstanding, the Commission did not deem this commitment sufficient, in particular, because the restricted data silo would cover only a part of data acquired by Fitbit.[21]

This is one of many examples of how certain commercial practices can raise concerns both from a competition (including the objective of consumer welfare) and data protection perspective. Further research and widely held policy discussions should support nuanced solutions to reconcile these perspectives in ways that protect fundamental rights, without completely curtailing innovation. The question at hand is most crucial as it may have long-lasting consequences on shaping future data use and protection issues, as shown by other notable mergers with an intense data-driven component.[22]

While data protection and competition law enforcement must not overlap, the two legal frameworks should not rigidly compartmentalize concerns that are, in fact, shared. The recognition that both policies pursue goals of fairness and self-determination for individuals should help devise concerted approaches to data-related matters. Cooperation among authorities is crucial, but it is also important to complement the authorities' resources (including staffing) with expertise from related fields.

As Mr. Buttarelli highlighted, there is an "osmosis of objectives"[23] between competition and data protection law, referring in particular to the decision by the German *Bundeskartellamt* on Facebook's practices regarding its users' personal data.[24] Importantly, he pleaded to shift attention to questions of fairness and choice in the digital economy.[25] As the next Section discusses, it is crucial for these purposes that individuals be recognized effective rights and remedies to rebalance power relationships in the market.

IV. Stakeholders and consumer collective redress

The GDPR enshrined the right to compensation for those who suffered material and non-material damage deriving from a GDPR violation.[26] Nevertheless, private GDPR damages actions remain, to date, limited due to the strains of in-court litigation, as well as cross-border divergences. Consumer and digital rights organizations allow a certain levelling of the power asymmetries that typically discourage individuals from taking action. There is strength in numbers, the saying goes. And especially when it comes to challenging large and powerful companies, possessing economic, manpower and expert resources is necessary to stand a fighting chance. As is well known, many landmark data protection cases,[27] and other collective redress initiatives,[28] originated from such organizations and greatly contributed to shaping the EU data protection framework.

---

[19] Case COMP/M.9660 *Google/Fitbit*. The deadline for the Commission's decision is 9 December 2020.

[20] "Commission opens in-depth investigation into the proposed acquisition of Fitbit by Google Brussels", 4 August 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1446. From a broader innovation and business perspective, it should be noted that data silos negate the true value of big data, i.e. re-usability for further analyses and processing.

[21] *Ibid*.

[22] Commission Decisions, Case COMP/M.4731 *Google/DoubleClick* (2008); Case COMP/M.7217, *Facebook/Whatsapp* (2014).

[23] G. Buttarelli, 'This Is Not an Article on Data Protection and Competition Law', *CPI Antitrust Chronicle*, February 2019, 3.

[24] "Bunderskartellamt prohibits Facebook from combining users' data from different sources," February 7, 2019. https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html.

[25] Buttarelli, *cit*., 'This Is Not an Article on Data Protection and Competition Law', 4.

[26] Art. 82(1), GDPR.

[27] CJEU, Case C-362/14 *Schrems I* (Judgment, 6 October 2015); Case C-311/18 *Schrems II* (Judgment, 16 July 2020); Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd* (Judgment, 8 April 2014); Case C-673/17 *Planet49 GmbH* (Judgment, 1 October 2019).

[28] Euroconsumer's class action against Facebook in the context of the Cambridge Analytica scandal, https://www.euroconsumers.org/activities/facebook-class-action-mydataismine-notyourpuppets.

Forthcoming legislation on consumer collective redress,[29] will harmonize and likely boost consumer class actions across the EU in coming years. The proposed measure, part of the "New Deal for Consumers",[30] grants standing to qualified entities, such as consumer organizations, to represent consumers in a variety of areas, including data protection.[31] The underlying rationale of granting individuals the power to act, for instance, both as a consumer *and* a data subject, supports a holistic approach to individuals' rights and forms of redress in the digital economy. It also suggests the possibility that the same action could lament multiple types of violations pursuant to different provisions of EU law but relating to one comprehensive abuse.

Moreover, GDPR-related class actions could constitute a game-changer in the EU. For instance, in 2019, the French CNIL received 14.137 complaints by individuals (27% increase compared to 2018 and 79% in five years);[32] the Italian *Garante Privacy* replied to 8.000 complaints;[33] 11.590 claims were filed with the Spanish AEPD;[34] while the Dutch *Autoriteit Persoonsgegevens* received 27.854 complaints.[35] The sheer numbers clearly indicate the great potential collective actions hold.

At this stage, Member States may be left to decide whether to provide an opt-in or opt-out mechanism,[36] therefore allowing some divergence on how an action may be adhered to. Opt-out constitutes an especially powerful tool for consumer organizations as consumers are automatically included, leading to a higher number of participants also thanks to inertia. As the numbers of complaints, notification of data breaches, fines imposed and inquiries steadily increase from year to year, cross-border data class actions are likely to soar under new harmonized rules.

In turn, this will increase litigation-related risks for data controllers, overall impacting the way business is done, raising the stakes for compliance, discouraging opaque or "borderline" practices. In this respect, a dialogue with industry stakeholders may help to identify key issues and facilitate compliance processes. In particular, resources should be considered to help small and medium size enterprises.

A balanced system requires all actors affected to be able to contribute and impact policy and practices. Broadly speaking, the EU's approach to policymaking, relying on thorough expert studies, stakeholder and public consultations, has the formal features of a fair dialogue. Accordingly, efforts should strive to improve wide and inclusive stakeholder participation and representation in these processes, as well as to ensure regular monitoring and *ex post* review of legislation.

Last but not least, effective data and consumer protection also require educational and cultural efforts on all parts, to improve digital literacy and privacy awareness, shifting from a "compliance-burden" mindset to the understanding of data protection as a shared value and an advantage for both individuals and businesses.

---

[29] General Secretariat of the Council, Directive of the European Parliament and of the Council on representative actions for the protection of the collective interests of consumers, and repealing Directive 2009/22/EC, 30 June 2020 ("CRD Text").

[30] Commission Communication, "A New Deal for Consumers", COM/2018/0183 final.

[31] Recital 6, CRD Text.

[32] "CNIL publishes its 2019 activity report", 9 June 2020, https://www.cnil.fr/fr/la-cnil-publie-son-rapport-dactivite-2019.

[33] "Relazione Attività 2019, Sintesi per la stampa", 23 June 2020, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9427952.

[34] "La notificación de quiebras de seguridad se triplica en 2019, consolidando la obligación establecida por el Reglamento", 4 May 2020, https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/la-notificacion-de-quiebras-de-seguridad-se-triplica-en-2019.

[35] "Annual report AP 2019: more focus on enforcement", 1 July 2020, https://autoriteitpersoonsgegevens.nl/nl/nieuws/jaarverslag-ap-2019-meer-focus-op-handhaving.

[36] Recital 15b, CRD Text.

V. Concluding remarks

An effective and beneficial relationship between consumers and their personal data is one relying on (effective) individual control. The example of data portability has shown the overlap and benefit of data protection and consumer rights. Effective control however must be paired with actionable rights and enforcement in each competent field. Going forward, a holistic approach to address data-related harmful practices in the digital economy is necessary.

The GDPR has given unprecedented powers to individuals: from the procedural right to lodge a complaint before a supervisory authority,[37] a set of actionable data subject rights,[38] to the general threat of fines as hefty as those of antitrust enforcement. New rules on collective consumer redress will further open opportunities for private data-related claims and ring a powerful warning.

***

Bibliography

Buttarelli, G. 'This Is Not an Article on Data Protection and Competition Law', *CPI Antitrust Chronicle*, February 2019.

De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., Sanchez, I., 'The right to data portability in the GDPR: Towards user-centric interoperability of digital services', *Computer Law & Security Review*, 34(2), 2018.

Engels, B. 'Data portability among online platforms', *Internet Policy Review*, 5(2), 2016.

Graef, I., Husovec, M, Purtova, N. 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law', Tilburg Law School Research Paper No. 2017/22.

Koops, B.J. 'The trouble with European Data Protection Law', *International Data Privacy Law*, 4(4), 2014.

Kuner, C., Cate, F.H., Millard, C., Svantesson, D.J.B., Lynskey, O. 'When two worlds collide: the interface between competition law and data protection', *International Data Privacy Law*, 4(4), 2014.

Lynskey, O. 'Aligning data protection rights with competition law remedies? The GDPR right to data portability', *European Law Review*, 42(6), 2017.

Purtova, N. *Property Rights in Personal Data. A European Perspective*, Wolters Kluwer, 2012.

Rodotà, S. 'Data Protection as a Fundamental Right', in (eds.) S. Gutwirth *et al*., *Reinventing Data Protection?*, Springer, 2009.

Somaini, L. 'The right to data portability and user control: ambitions and limitations', *MediaLaws – Rivista di diritto dei media*, 3, 2018.

Swire P., Lagos, Y. 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique', *Maryland Law Review*, 72(2), 2013.

van Ooijen, I., Vrabec, H.U. 'Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective, *Journal of Consumer Policy*, 42(91), 2019.

***

[37] Article 77, GDPR.

[38] Articles 12-22, GDPR.